UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,736	06/29/2001	Karanvir Grewal	P 0275038 P11033	3327

7590 10/23/2003

Pillsbury Winthrop LLP
1600 Tysons Blvd.
McLean, VA 22102

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	6

DATE MAILED: 10/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/893,736	GREWAL ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 0201* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☑ Claim(s) *1-17 and 19-30* is/are rejected.

7)☒ Claim(s) *18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☑ The drawing(s) filed on *6/29/01* is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-30 are pending for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 1, 3-7, 9-18, 21-30 are rejected under 35 U.S.C. 102(b) as being anticipated by D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", Request for Comments (2409), published 1998.

As per claims 1, 3-7, 23, RFC 2409 (IDS #5) describes a hybrid protocol (IKE) providing authenticated keying material for, security associations in a protected manner, see abstract.

RFC 2409 fully discloses processes for implementing negotiating virtual private network (VPN) and also providing a remote user (i.e. first peer) from a remote site access to a secure host or network (i.e. second peer), see page 2, 2nd paragraph in Discussion section.

RFC 2409 Hybrid protocol employs part of Oakley and part of SKEME in conjunction with ISAKMP (Internet Security Association and Key management protocol) to obtain authenticated keying material for ISAKMP, and for other security associations such as AH and ESP for IPsec protocol, see Abstract, third paragraph.

That is, IKE (RFC 2409) presents exchanges as modes (described in Oakley) operating in one of two phases defined in ISAKMP, see page 3, Introduction.

Phase 1 (or preliminary negotiation) where two ISAKMP peers establish a secure, authenticated channel with which to communicate (i.e. a security association, SA). RFC 2409 discloses that " Main mode" and " Aggressive Mode" each accomplish a phase one exchange.

Phase 2 where security associations are negotiated on behalf of service such as IPsec or any other service which needs key material and/or parameters negotiation. RFC 2409 describes that "Quick Mode" accomplishes a phase 2 exchange.

As per claims 9-10 and 17 and 24, RFC 409 described that during Security Association negotiation (i.e. setting policy information at phase 1 of IKE) initiators present offers (proposals) for potential security associations, see page 9, paragraphs 6 and 7, and that there is no limit on the number of offers (i.e. number of security associations) the initiator may send to the responder.

As per claim 11, RFC 2409 discloses attributes including security parameters and network addresses negotiated as part of the security association, see page 6, 5th paragraph, through page 7, first paragraph, where all the attributes are mandatory and must be negotiated.

As per claims 12- 14, RFC 2409 discloses that the in Quick mode (at Phase 2) an optional key exchange payload cab be exchanged to allow for an additional Diffie-Hellman exchange (i.e. to generate a secure key), see page 17, paragraphs 2-3.

As per claims 15 and 16, RFC 2409 teaches an identification payload (i.e. an IP address) for initiator or responder during Phase one negotiation, see page 4, 2nd paragraph.

RFC 2409 further discloses Phase 1 authenticated with a pre-shared key, see page 16, wherein a key derived by some out-of-band mechanism (or stored) may also be used to

authenticate the exchange and that the pre-shared key can only be identified by IP address of the peers.

As per claim 18, RFC 2409 discloses that Main mode, Aggressive Mode, and Quick Mode do security association negotiation and that the security association offers take the form of Transform Payload(s) encapsulated in proposal payload(s) encapsulated in Security Association payload(s)and if multiple offers are being made for phase 1 exchanges they must take the form of multiple Transform payloads for a single proposal payload in a single SA payload.

Claim 21 recites limitations of claim 5. It is rejected for the same reasons states in the rejection of claim 5 above.

As per claim 22, IKE (RFC 2409) presents exchanges as modes (described in Oakley) operating in one of two phases defined in ISAKMP, see page 3, Introduction.

Phase 1 (or preliminary negotiation) where two ISAKMP peers establish a secure, authenticated channel with which to communicate (i.e. a security association, SA). RFC 2409 discloses that " Main mode" and " Aggressive Mode" each accomplish a phase one exchange, see page 5, section 4.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 8, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable D. Harkins, D. Carrel as applied in claims 2 and 6 and further in view of D. Dukes, R. Pereira, "ISAKMP Configuration Method", The Internet-Draft, March 2000 and further in view of Y. Dayan, S. Bitan, "IKE Base Mode", Internet-Draft, January 2000.

As per claims 2 and 8, The ISAKMP Configuration method (IDS#5) discloses a new ISAKMP configuration method to allow IPsec-enabled entities to acquire and share configuration information, see page 11, section 7. That is, retrieving certain information from the other peer before the non-ISAKMP SA can be established is sometimes useful, see page 3, section 1.

As per claims 19 and 20, IKE Base mode (IDS#5) describes a new phase 1 mode that is based on the ISAKMP Base Exchange, see page 2, 4th paragraph. In the Base mode Exchange, the first two messages negotiate policy, exchange ancillary data necessary for the exchange, and the identities (recited in claim 20). It would have been obvious to employ the IKE base mode in place of Main mode and/or the Aggressive mode of the IKE protocol when the either the IP address does not identify the peer (in case of Main mode) or if the identities appear in the first messages (in case of Aggressive mode) leaves the responder exposed to denial of service, see page 2, third paragraph.

Allowable Subject Matter

Claim 18 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

Taghi Arani

Patent Examiner

October 15, 2003.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100